A PROPER PERSPECTIVE OF PRIVACY LAWS
WHAT MANAGERS NEED TO KNOW ABOUT PRIVACY LAW

AFONSO NETO
DOCUMENT ACCESS LEVEL:

The information expressed in this document is property of Cipher. Although it can be disclosed, distributed, copied, read, used, printed or accessed by anyone, as long as all the Cipher credits are respected. The previous statement is protected by the effective law.
REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision Overview</th>
<th>Reviewers</th>
</tr>
</thead>
<tbody>
<tr>
<td>30-12-2019</td>
<td>First draft.</td>
<td>Afonso Neto</td>
</tr>
<tr>
<td>13-05-2020</td>
<td>Review pointing technical improvements.</td>
<td>Afonso Neto</td>
</tr>
<tr>
<td>10-07-2020</td>
<td>General technical review.</td>
<td>Miguel Brown</td>
</tr>
<tr>
<td>21-07-2020</td>
<td>Detailed revision proposing some details about Privacy Laws in United States.</td>
<td>William Bowman and David Rickard</td>
</tr>
<tr>
<td>03-08-2020</td>
<td>Last general review</td>
<td>Afonso Neto</td>
</tr>
<tr>
<td>04-08-2020</td>
<td>Final Version</td>
<td>Afonso Neto</td>
</tr>
</tbody>
</table>

ACRONYMS

CA - California
CCPA - California Consumer Privacy Act
DPIA - Data Privacy Impact Assessments
EU - European Union
GDPR - General Data Protection Regulation
GRC - Governance, Risk Management and Compliance
HIPAA - Health Insurance Portability and Accountability Act
US - United States
Ensuring privacy is becoming an ever increasing obligation. In the current pandemic - where a significant amount of work is undertaken remotely, organizations must not only be aware of privacy laws, but clients, collaborators and employees too, have to understand that privacy is not a commodity organizations can treat lightly. Personal privacy must be respected no matter what. This necessity has been fostered by the invasive turn that current technological advances are taking, and the abuse that is visibly coming along with it.

Today we are seeing a global boom of new privacy laws and, where they already existed, they are being strengthened. A good example of this is the case of the General Data Protection Regulation - GDPR - in Europe, which in 2016 replaced the 1997 Data Privacy Directive. Governance, Risk Management and Compliance (GRC) initiatives are now obliged to embed privacy concerns in their already complicated risk and information security requirements spectrum. At the same time they need to attend to all matters required by existing local laws, such as restrictions to video surveillance and labor relationship obligations.

For instance, in Portugal, strict rules already exist to regulate in which circumstances an employer can access a company owned employees email inbox. As this is assumed to contain personal information, the reality is that the organization is not free to use its own resources as it pleases anymore.

When assisting organizations to tackle their privacy challenges, one thing that emerges is that managers are often confused not only by the details of the laws and regulations, but also by what such complex regulations are trying to accomplish. Basically, it is not obvious why they cannot still freely use information that is clearly owned by the organization, even when this information is created and processed by their own employees during the course of their work. In essence, what becomes clear is that there remains a misunderstanding about the deep meaning of what privacy really is. The laws and regulations are extremely complex, but this is due to the fact that privacy is a complex issue, much more complex than merely labelling information as confidential or secret.

Understanding privacy correctly actually makes attending to privacy laws and regulations much easier.
A mistake often made by managers is to try and understand privacy as a simple confidentiality requirement, which is not correct. Privacy should not be seen as the same as the keeping of secrets, even if confidentiality, as an information security requirement, can be used to enforce privacy.

Privacy is better understood as the requirement to prevent the psychologically negative effect of being watched and, because of that, the feeling of being judged by other people on an individual and personal level. When protecting privacy, the goal of the legislator will be to assure that under no circumstance people feel as if they are being evaluated with regard to situations, actions and knowledge that they don’t want and in situations where they should not be. No such situations or knowledge have to be particularly secret or illegal for the person to want to keep them private, and therefore the core of privacy comes from something strictly personal, varies immensely from person to person, depends significantly on cultural background, and ultimately is so subjective that even individuals themselves have a hard time explaining what they really want and why.

Understanding this perspective is a game-changer when it comes to realizing why the laws are organized in the way they are and, more importantly, how the provisions of the laws (such as consent) can be effectively and correctly attended to.

In this essay we will examine the main characteristics found in most Personal Data Laws around the world and analyse them through the lens of this new way of interpreting privacy: the protection against the uncomfortable feeling of needlessly being judged on a personal level. This perspective is easier to grasp and allows for the straightforward derivation of most legislative requirements imposed on today’s organizations.

1. UNDERSTANDING THE DEFINITION OF PERSONAL DATA

Each different legislation gives a different definition for personal data, even though they all try to achieve the same goal: to include everything that is personal and what people might have concerns about sharing, even without having the condition of identifying exactly what and why.
The goal of the legislator will be to devise a definition that captures all kinds of data and information that few people might have concerns about, and this is clearly difficult to do. This exercise invariably leads to the realization that almost any information that points to an action or characteristic of an individual person, or event involving them, will be of concern to someone. Because of this, the only option is that laws should abstain from trying to decide for them, beforehand, what is important to keep private or not. Ultimately, the decision of what matters will have to be a personal unquestionable decision, and therefore, for information to be personal data it is enough that it is related to a private individual.

This is the first error most managers often make, which is to assume that their own perspective of privacy - of what they personally care about and want to be private or not - will be the same for all other individuals, in particular their employees. Data protection laws start by stating that managers cannot impose their own personal vision of data privacy on others, even if in other circumstances they would have power to do so.

When it comes to personal data classification, the only thing we typically encounter in more specific terms is a subset of personal data that is universally considered to have a higher critical status, and this is only because of already known negative impacts their exploitation might cause to their owners. Among this specific information we can find health and biometric information, and religious and sexual preferences, for example. This set may vary from country to country as, for example, financial information might be considered critical for some and not critical for others, in particular, when other interests are at stake.

In summary, if information points to a singular individual, then it is personal data. If it used to point to someone, but the connection is lost and cannot be recovered, then it is anonymized personal data. If it does not point to any singular individual at all, then it is not personal data. Pseudonymity is a term used when the connection to an individual exists, but is in general concealed, available only under strict circumstances.

It is important to note a significant effect of such an approach to this definition: personal data is not always owned by the individual it points to. This is a fact which causes real confusion to managers, but it becomes clear if we assume that it is not hard for organizations to know more things about people than they themselves know (through correlation, for instance). However, regardless of who owns the data, if the data points to a singular individual - then this person has a say on what can be done with it. Nevertheless, the powers that the individual has over his or her personal data are in reality quite limited, and far from absolute, as we analyze in the following sections.

2. UNDERSTANDING LAWFULLNESS

Data protection laws will usually provide a list of possible justifications to process personal data, and any personal data processing must abide by one of the presented reasons. We refer to such reasons as “lawful grounds”, and they are the way the laws clarify when is it acceptable to process personal data. The list establishes what is allowed and, therefore, when a certain processing cannot be justified by one of the lawful grounds on the list, this is when it is considered illegal. To reinforce this effect, several regulatory bodies opted to include heavy fines for unlawful operations in their legislation. Interestingly, all these lists (independently of their specific arrangements) can be analyzed from a simpler perspective, which will help in their overall understanding.
Irrespective of what legislation we are considering, whenever privacy is being protected, there are only two acceptable reasons for processing personal data: either the individual clearly wants the data to be processed or there is a more relevant issue at stake that must override the person’s individual concerns regarding his or her privacy. In both cases, the legislators understand that privacy is not set in stone, and there may be legitimate reasons for breaking privacy whenever benefits can be reaped from it.

**Consent** is the name usually given to the effective expression of someone allowing his or her data to be processed. It usually requires a record of some sort (electronic or otherwise) with a structure that demonstrates, as clearly as possible, that communicates what the process entails so that the person involved understands what will happen with the data. This is one way of making processing of personal data lawful.

Another common way for people to express their agreement to having their personal data processed is exercised in the form of **contracts**. Whenever a contract is settled, usually we will find it brings advantages for both signatory parties and, when one of them is an individual, then having their data processed may be a requirement for having their own advantage realized. This is the general case with the provision of services, as well as for employment contracts which, for the employee to actually execute the employment role, he or she must have his or her own personal data processed to some extent. For this reason, the execution of contracts is another common lawful ground for processing, which therefore will not require a formal separate consent register. In such cases, the consent is implicit because the individual wants to be a part of the contract and exercising the contract requires the processing of his own personal data.

In both cases - consent or contract - if the processing is undertaken because the owner of the personal data is agreeable to it, this allows us to assume that this individual has evaluated all the consequences of the processing and that he or she does not feel they are being unnecessarily judged or have cause to be embarrassed. However, one caveat is that this is only true if the person has all the information about the processing that is about to take place and, also, that he or she was not coerced in any way. In addition, he or she must be provided with a general assessment of potential risks in the necessary exposure of their data to third parties that may be involved. In any case, we can accept that the person gave their express authorization whenever they were not forced to enter into the contract (or obliged to accept particular clauses pertaining to it) or, similarly, if they freely signed a consent form that is clear, direct and complete.
The second major situation where we might have lawful grounds for processing personal data is when an issue is at stake that is far beyond the need for the agreement of the individual. We suggest, for example, two common kinds of situations where the agreement of the individual may be overridden: public interest and private groups interests.

More often than not, public interest is manifested through laws and regulations. This is why, almost by definition, whenever some law requires personal data processing, this processing is lawful regardless of the will of the individual. The idea is that society as a whole has already determined that it needs this processing to occur, and no amount of personal subjectivity should prevent it from doing so. Areas where this applies might be with taxes and public welfare systems for example. In such cases, the real challenge will be devising the processing steps in a way that the processing accomplishes only what the legislators expect and nothing more. For example, public officials building cross-relational databases in order to “accelerate” public services might be acting unlawfully if not authorized beforehand though some other mechanism. Processing is not lawful merely because the government is doing it, but only because there is some law that requires it and the goal of the processing is directly tied to the goal of the original law, nothing more. This is often overlooked by public officials.

In a similar way, additional types of data processing can in general be considered necessary for societies, and override individual judgment, even if there are no explicit laws with regard to them. Medical emergencies, historical archiving of important information and freedom of speech and of the press are some examples. When there is a lack of specific clear legislation, such cases will usually be found directly in the data protection laws, in order to avoid legal disputes or unnecessary complications.

Private groups, such as independent organizations and private corporations, are another matter. There are several reasons they might need to process personal data and such reasons might not be in the direct interest of the data subjects nor be predicted by law, but otherwise might make sense for the sake of the organizations themselves. For example, under GDPR, we call such reasons the “legitimate interests” of the organization and the way GDPR was structured makes it an obligation for the organization to clearly demonstrate that the interests of such processing are legitimate and should override the rights of particular individuals.

One common case is processing for security purposes (be it physical security with video-cameras or cybersecurity with firewalls and intrusion detection). In such situations, the idea is that the security of the whole organization cannot be jeopardized because one person does not want to have his or her information processed. In such circumstances it is fine to give up some of the privacy of the individuals in order to assure security. Nevertheless, it is expected that the individuals are informed of the processing that is occurring and that they are given the opportunity to challenge such interests if they do not agree with them.

In summary, lawfulness of processing is the method legislators have available to create a line that clearly demands that privacy should be absolute unless explicitly and formally given up, either by the individual or by a legitimate requirement of a group (society or otherwise). Because it is not feasible to simply address the question “is this processing acceptable for this particular person?” for all individuals at all times, then, looking for a lawful ground within the data protection law will be the preferred method of accomplishing the same task.
3. UNDERSTANDING TRANSPARENCY

Simply put, transparency is a direct consequence of lawfulness. When it comes to personal data processing, transparency will be required in many different ways, most of them without mentioning it explicitly. It is important to note that a lack of transparency can effectively nullify the lawful grounds being used to justify processing, so organizations must be careful.

The idea is that, in all cases, when personal data processing is taking place then some privacy is being taken away. This will only be acceptable (therefore lawful) if either the person is agreeable to it explicitly or if some other issue beyond the agreement of the individual has been clearly established. The only way an individual has the chance of knowing if his privacy loss is legitimate under the law is if he knows all the details of what is being done with his information and what the reasons are that allow for it. Because of this, the data protection laws require that this communication must be made explicitly, often written (but not always), and they must occur in some way so that it becomes unquestionable that the individual knows what is going on.

Full transparency is required in all cases, independently of the reason that justifies the processing. This includes consent, contracts and legitimate interests and, even if disputable, processing based on other laws. Without the full knowledge of the individual, it is not possible to ensure that all the conditions of lawfulness have been addressed, and acceptability of breach of privacy has been established. Transparency will often include information regarding the security measures involved in the process, for the same reasons.

4. UNDERSTANDING PERSONAL DATA RIGHTS

Once a particular data processing is considered lawful and the data subject is agreeable to it, this does not mean that the data becomes the property of the organization processing it. Given the characteristics of the processing, the data subject can still intervene in the process and the rights that he or she has are the mechanisms the legislation provides to do exactly that.

One common right is that which allows a person to simply change his mind about the processing and remove his authorization, which seems reasonable. However, this has several limitations, for good reasons.
When the lawful ground is a simple consent, then the organization usually must allow for the person to express his change of mind easily and the processing must stop immediately. Nevertheless, such provision does not exist when the ground is the execution of a contract, and the ceasing of personal data processing in such cases only occurs under the same circumstances that the general laws allow for the contract to be terminated. Even when the contract comes to an end, there might be reasons for additional processing (to keep records about what happened) and to comply with additional laws.

In other situations, there might be reasons where the ceasing of the processing might cause damage to third parties and therefore can be denied because of that. This is the reason where most consultants will recommend avoiding consent as lawful grounds to processing when other justifications are available and, also, why asking consent of employees is a bad idea.

Other typical rights will include “good sense” provisions, such as knowledge about the processing and its consequences, transfers that may occur, the ability to know exactly what data the organization has, the ability to update the data when it is outdated and the possibility of asking for the data to be deleted if no good reason for keeping it exists. Data protection rights are also another example of the way legislators found to translate options that are only subjectively defined into objective measurable features that are not more than reasonable expectations.

One right that is popular and does not follow such simple pattern is the portability right (GDPR in Europe and LGPD in Brazil), the origin of which might not be as obvious as we would expect. This right came forth from the characteristics of specific technological services (such as telecommunications), and the idea that changing providers of such services should be something easy to do, in particular, if a good amount of personal data is involved in the change.

From this basic, simple idea, the right was generalized, in order to not prevent potential advantages in different areas and to remain relevant depending upon how the information technology services will evolve in the future. The idea is that some types of data are so intrinsically tied to the services being provided that it would be sensible that organizations themselves would facilitate for customers the change of provider if they want to, and therefore the portability right was born. This right is one example of an idiosyncrasy that is not directly derived from personal data protection, but has come to stay.
5. UNDERSTANDING DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default is better understood as two distinct objectives, each with very clear consequences. We shall refer to them as security by design and privacy by default, and each of them are often present in legislation in one way or another. The best way to comprehend those requirements is to understand that they are not mere desires of the legislators - of course we want the data to be secure and private - but are fundamentally tied to transparency and lawfulness.

When we communicate what will be done with a particular personal data set and collect the acknowledgment of the data subjects (implicitly or explicitly) we are establishing the lawfulness of the processing. However, this comes with an implicit agreement that what was communicated is the whole extent of the processing, and that the organization will take steps that assure that no additional and secondary “hidden” processing will occur. This should be obvious because no processing can occur without transparency and lawful grounds.

It is reasonable to expect that an honest organization will not carry out illicit actions wilfully, and this should go without saying. However, in today’s technological landscape, taking steps to assure that no malicious individual can subvert a correctly defined process is another matter entirely, and one that cannot be neglected. This means that the way the organization will carry out the processing must be resilient and secure even when we consider malicious individuals that decide that they will take advantage of it. An information security incident with personal data is not only an illegal act of the perpetrator, it is also a violation of the lawful grounds of processing between the organization and the data subject, because now additional unauthorized processing has occurred. A process will only be acceptable if it takes the possibility of this violation seriously, and takes effective steps to prevent it.

This is actually the gist of security by design, which means that the definition of the processing steps include all reasonable precautions against malicious attacks, be it from external hackers or from insider threats, and therefore the data is protected against attacks. Basically, the data subject will accept the processing given the assumption that he is not incurring unacceptable risks, notwithstanding that some level of risk always exist. This is reasonable and any subject can expect this to be the case. Security of processes, by design, is the only way to honor such expectations.
Notice that security by design also has consequences on its own and gives rise to several additional requirements present in most laws and regulations. Keeping records of processing activities, having a security incident handling process, assuring the communication of incidents to data subjects and data protection authorities, the assignment of data controllers and processors responsibilities, data protection impact assessments and prior consultation are examples - under GDPR - of such expectations. And yet, they are all naturally derived from the unique way legislators have chosen to ensure that privacy is protected.

Privacy by default, on the other hand, is another concept that is frequently present in legislation but is not the same as security by design. Privacy by default is relevant when processing may occur according to different levels of invasiveness (i.e. privacy loss), and there are optional features that the data subject can select from within the same service. Take for instance a mobile phone that may also capture geolocation information. Functionalties allowed by geolocation might be extremely useful and desirable by most users, but they all come with the loss of privacy to some extent, and therefore must not occur unless lawfulness is assured.

**Privacy by default** is the idea that the organization must assume, when a user is consenting to a service, that the only authorization he is giving is in respect to the lowest level of privacy loss available. The additional levels of privacy loss, if they exist, should only occur according to proper steps of transparency and communication, and this is complex to do in a clear way if the levels of privacy loss are all intertwined. This invariably happens when a service is activated with all the optional features - that have an impact on privacy - turned on. To solve this, data protection laws will establish that such options must be turned off from the start (by default) so the user can clearly evaluate each individual level of impact and assess if he or she does or does not want to give up his or her information given the advantages provided, if any.

Notice that privacy by default is also another consequence of the way lawfulness is defined. The fact that the user can turn off the options later is not enough because if the person does not want to have this data to be processed, then during the time between activating the service and the action of turning the optional service off, all the processing that occurred in between is illegal and therefore must be prevented. This is always true, and we are not even considering that it is common that users are not aware of the “additional” options, or how to turn them off. **Personal data protection can only be assured with privacy by default, and there is no other way to achieve this correctly.**

### 6. PRIVACY LAW IN THE UNITED STATES

In the United States, privacy law and the controversy surrounding privacy has a history and complexity beyond the scope of this paper. In 2001, the Patriot Act brought privacy to the public debate, as safety and privacy were balanced in the War on Terrorism. The provisions of the act have all expired now, but the controversy regarding Government data collection persists. Medical data has been protected by Health Insurance Portability and Accountability Act (HIPAA) since 1996. On the business side, GDPR has impacted many companies in the United States. Companies that do business in the European Union have changed policies to adapt. The item that any person online might notice is increasing statements about cookies on websites. Companies that do business globally are adapting to meet the guidelines of the regulations in order to avoid penalty.

Individual states within the US have also created privacy frameworks and laws to protect their citizens. Nevada and Maine both have laws that require companies doing business in their state to
follow certain rules. Many other states are in the process of drafting laws. California has maintained the California Consumer Privacy Act (CCPA) since early 2020. With California being the largest state, its law has attracted the most attention.

Comparing GDPR to CCPA will allow us to see if a company can satisfy both laws using similar processes. GDPR is more comprehensive and restrictive than CCPA. Companies could modify GDPR to suit a CCPA regulations in some cases. We recommend that companies focus on becoming GDPR compliant first and then determine if those processes satisfy CCPA compliance. There are some important differences between GDPR and CCPA that are worth noting however. There are differences in the scope of who the regulation relates to. GDPR pertains to all EU citizens (“data subjects”) while CCPA pertains only to CA residents (“consumers”). CCPA only applies to businesses that do business in California and meet on of the following criteria. If they have $25,000,000 or more in annual revenue, buys and/or sells information of 50,000 records for people in California or derive more than half of their revenue from selling private information, they must comply. GDPR applies to individual data subjects only without regard for how much a business makes or where it is.

Time periods and guidance for accessing criteria is different. GDPR allows for Subject Access Requests that must be fulfilled in 30 days. CCPA allows 45 days for fulfillment, with a possible 45-day extension. GDPR and CCPA both have data subject/consumer rights of erasure. CCPA has more exceptions that would allow a business to decline the request, and pertains only to personally identifiable information that the consumer provided directly to the business.

Fines related to each differ. GDPR maximum fines are 4% of gross annual revenue or €20,000,000, whichever is greater. The fine can be imposed as a result of audit and non-compliance. CCPA imposes fines up to $7,500 USD per violation and only if the data is breached.

Other elements also differ. CCPA is focused on the sale of consumer information. GDPR is focused on the collection and processing of data subject information whether or not it’s sold. GDPR requires Data Process Flow Mapping and predetermined amount of risk to data per business process that involves privacy data. CCPA doesn’t require that, and specifies nothing about Data Privacy Impact Assessments (DPIA).

While GDPR could further evolve, it’s been essentially the same since submitted in 2016 and going into effect in 2018. CCPA could change as it starts being applied.
7. TRANSATLANTIC PRIVACY AGREEMENTS

In July 2016, the European Union and United States agreed on a framework for sharing citizen personal data known as Privacy Shield. The Privacy Shield was meant to make data transfer between the United States and European Union countries easier. Over 5,000 businesses enrolled in the Privacy Shield in the United States.

Before the agreement was in place, companies were bound to Safe Harbor, which took effect in 2000. Methods to get data from EU citizens into the United States were even more onerous before Safe Harbor, with companies making deals on a one-off basis to get data out.

Critics argued that the laws and privacy guidelines in the United States made data on EU citizens vulnerable to breach or misuse. Maximilian Schrems and his NOYB group, in particular, campaigned for strict privacy for EU citizens. In July 2020, a court struck down the agreement. The court asserted that the United States could not properly safeguard the personal data of Europeans.

US Senators Roger Wicker and Jerry Moran said in a statement: “The economic effect of invalidating the EU-U.S. Privacy Shield, particularly on small and medium-sized businesses, is troubling,” said Wicker and Moran. “This would cause significant disruptions to data transfers and trade activity between the EU and the United States. We need to work quickly to establish a successor framework that supports economic development and adequately protects consumer data across borders.”

Until a new agreement is reached, there will be uncertainty with regards to data privacy laws and enforcement. It is unknown if the governments can agree on a new framework or whether compliance will be enforced or if there will be a grace period. Companies might be forced to make arrangements to transfer data on a case-by-case basis.
FINAL THOUGHTS

Complying with laws may sometimes be hard, but accomplishing personal data protection should not be so difficult. To demonstrate why, we described the main elements of almost all data protection laws in the world taking advantage only of good sense and reasonable expectations given our current technological situation. Applying rationales that are easy to grasp and relate to, one can lead an organization almost completely in compliance without having to consider a single article of the legislation and, better yet, such compliance will work with almost all of the laws and regulations in existence, automatically and simultaneously.

This is not to say that implementing compliance with data protection laws is always easy, which it is not, but to show that understanding the path to compliance need not be overly complex. The trick is to analyze the situations from the correct perspective, and maybe answer a simple question:

“What would YOU expect if it was YOUR data we were talking about?”.